Data Protection Officer Guidance for Microsoft Teams

Version:	1.0
Document Lead:	Graeme Temblett-Willis – Data Protection Officer Dominique Emmanuel– Informatics Training Manager
Category:	Microsoft Teams (MS Teams) Technology
Date Issued:	17/06/2020
Review Date:	16/06/2020
Approved Date:	
Approval Committee	COVID-19 necessity (IGG June 2020 for review)
Target Audience:	All staff (permanent and temporary) All associate staff Contractors

Contents

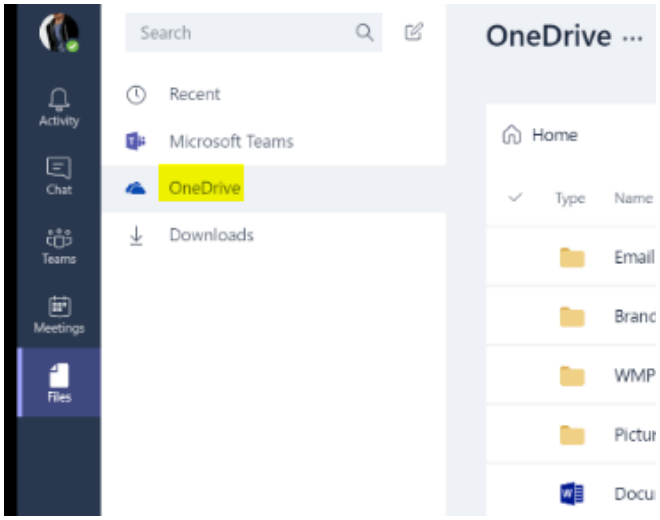
Introduction

The introduction of Microsoft Teams creates efficiencies in the streamlining of communication and implementing remote working capabilities. Microsoft Teams and its integration with many other Office365 apps has been approved by NHS Digital.

How to Upload/Share files on Microsoft Teams

Microsoft Teams allows users and teams to upload files in a secure file structure. This involves both a personal 'OneDrive' file storage (which is roughly equivalent to a user's personal 'P: Drive' on their Trust desktop). It also includes structured file sharing across 'Teams' of Trust staff.

Personal Files – A user is able to store files that are visible and accessible only by himself/herself via OneDrive. Storing files onto OneDrive is the equivalent to storing a file on to a local 'personal drive' (i.e., a 'P:' drive):

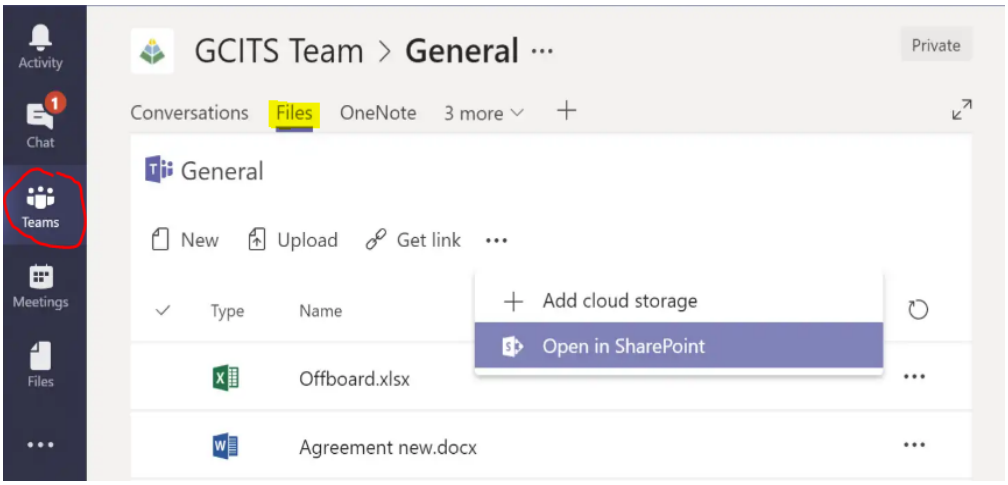


Shared Files and Team Structures: – Users may store files on a designated private 'Team' which is a shared environment. These files will be accessible by all members within the team via SharePoint. This 'Team' tab provides the functionality to serve as central repositories for information required to be shared between members of a team.

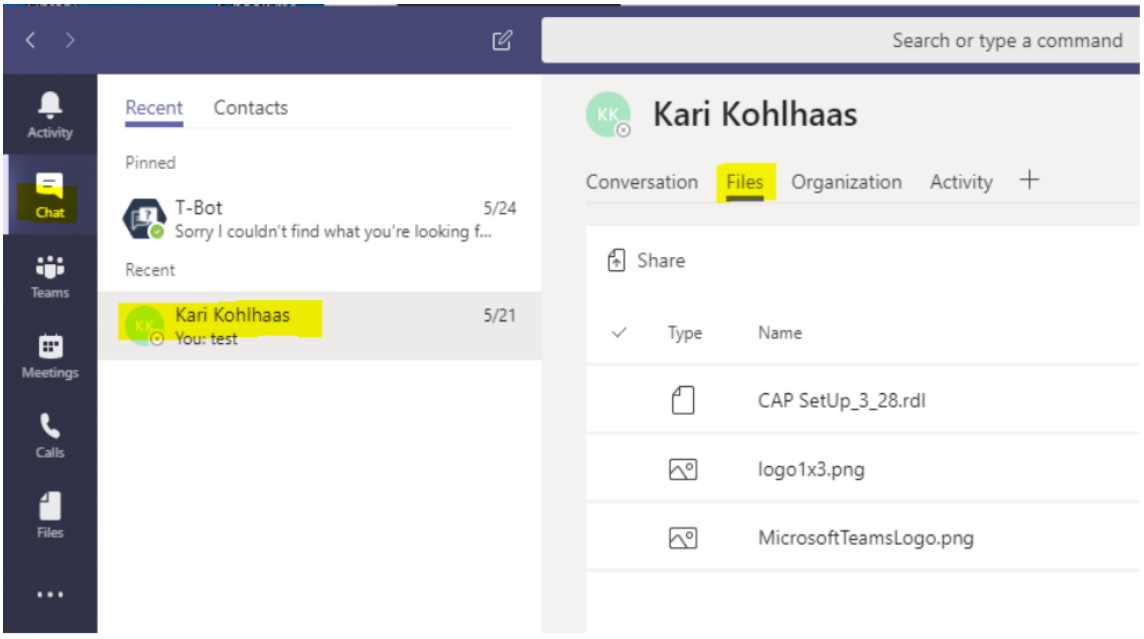
It is RUH Bath Trust policy and IG advice, that files containing confidential or patient / staff identifiable information should not remain stored on MS teams after the original discussion after the chat, meeting or video call, but removed and stored in line with NHS Records Retention Codes of Practice and the Data Protection Principles in the normal manner using the departmental secure file structure already in existence.

The Data Protection Principles and GDPR legislation can be found at the following link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

The Records retention Codes of Practice can be found at the following link https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016



Sharing files over ad hoc chats**:** Files may also be shared outside of a team within a 'chat' environment where files will be visible, available and accessible by all members within the 'chat' via SharePoint. Chats may be established with any other member of the organisation, allowing Trust staff to share files across different divisions, departments etc. Sharing a file on an individual chat will lead to a SharePoint being established within that chat's environment.



A '**Team'** and/or a '**Chat'** on Microsoft Teams allows members to collectively work on and store files on a shared environment via SharePoint (i.e., in a manner comparable to a shared drive). Therefore, managers must be aware that every '**Team'** and '**Chat'** member will have visibility of the uploaded files.

Storing files on a '**Team'** SharePoint is the equivalent of saving a file onto a local 'shared drive' (i.e., an 'S:' drive). **It is recommended that the Team SharePoint is used as the primary file structure for your team's documents. However, attention must be made to removing and storing / deleting as stated previously in this document from the SharePoint as this will ensure there is greater control over access and appropriate data sharing in**

accordance with the data protection principles. It will also assist in archiving and auditing during the information risk management process that is completed annually.

Sharing files over an individual '**Chat'** is similar to sharing a document over email as an attachment, except that all members of that chat group have visibility and write-access to the files shared. **It is recommended that files shared over Chats are worked on in situ and then stored centrally in the relevant Team file structure**

It is important to remember that whenever a file is shared over a Team or Chat group, it is available and accessible to all members of that group. Therefore, Trust staff **must** be mindful of the data being shared and the appropriateness of access being provided to these staff. Data shared should be minimal for the purposes of sharing and access limited to those that require it.

Data Sharing Principles

Where appropriate, Trust staff **may** use Teams for clinical use, up to and including the sharing of patient identifiable information, on the understanding that the application has appropriate technical and organisational security controls in place.

However, all Trust policies apply to the use of data on the Teams platform. This necessitates that **no** patient identifiable or otherwise commercially sensitive information may be downloaded onto a personal computer outside of the Trust network for **any** reason.

Trust staff are also expected to recognise and uphold the Data Protection Principles concerning data minimisation, purpose limitation, and control of access to patient identifiable data. This requires that data is not shared beyond a need-to-know basis, and only the minimum information is shared to satisfy the specific purposes of its use.

Microsoft Teams applications Integration

Table 1 – Available drives:

Drive	Trust Infrastructure Equivalent	Cloud Infrastructure
Personal Drive	P: Drive	OneDrive
Shared Drive	S: Drive	SharePoint

NB: There is no interface between the Trust Infrastructure and the Cloud Infrastructure and this means OneDrive / SharePoint will be completely empty at the starting point and will have to be populated.

Microsoft Teams applications integrate into the approved cloud infrastructure drives. This means that data generated using the various Microsoft Teams applications approved below will be saved in the respective cloud infrastructure drive.

Off-sited teams will need to migrate files held in the S: Drive to Microsoft Teams SharePoint folders, where it is not possible to access these in parallel using remote access / VDI. Microsoft Teams SharePoint and the Trust Network file structure **are distinct and exist in parallel to one another**. Therefore, off-sited teams must consider carefully their approach to file management and how best to make documents available to staff without access to the Trust Network.

It is recommended that robust and organised file structures be implemented when using Microsoft Teams SharePoint. This should include numbered and tiered file structures. Procedures and enforcement to maintain the tiered and organised file structure in good logical

working order (i.e., new folders must only be created/deleted by agreement with management and this must be kept under review). In the longer term, the DPO recommends that there is an annual archiving procedure to ensure that files are well-ordered and structured and can be retrieved easily.

Joiners, Movers and Leavers processes must be followed in all instances when using Microsoft Teams with regards to file management structure. This means that responsibility must always be assigned to a current and appropriate member of staff for the management of file shares and the personal drives (i.e., OneDrive) of any leavers must be sanitised as appropriate to avoid data leakage where these leavers move to other NHS Organisations.

All file shares should have at least two administrators to prevent a single point of failure in the management of SharePoint.

Information Risk Management (IRM) and Information Asset Owners / Administrators (IAO / IAA).

It is essential and a requirement under GDPR that records of identifiable data are appropriately and accurately controlled. In order for the Trust to be compliant with this, each department must ensure that there are two nominated IAA's (Information Asset Administrator/s) and that the MS Team lead is the designated IAO (Information Asset Owner). The details of these members of staff must be passed to the IG Team so that the IRM audit records can be kept. The IG Team will ensure that support and guidance is provided to the team IAO's and IAA's so that this is not a burden to them, but does enable the Trust to provide assurance to the SIRO (Interim Chief Executive Officer) and Board of GDPR compliance. Contact for the IG Team can be made via ruh-tr.IGQueries@nhs.net

It is important to remember that the IG Team are available as advisors in relation to the data elements of MS Teams and not in relation to technical difficulties that may be encountered during deployment or use of the platform.

Further Information, FAQs and Guidance:

The above guidance represents how Microsoft Teams should be deployed by your Team for use within the Trust. For more general information on Teams and Office365 functionality, please consult NHS Digital's guidance at the following links:

https://support.nhs.net/article-categories/teams/ (Microsoft Teams)
https://support.nhs.net/article-categories/using-o365/ (Office365)